Parameterization of Boolean functions by vectorial functions and associated constructions

Claude Carlet,

University of Bergen, Norway; University of Paris 8, France.
E-mail: claude.carlet@gmail.com

Despite intensive research on Boolean functions for cryptography for over thirty years, there are very few known general constructions allowing to satisfy all the necessary criteria for ensuring the resistance against all the main known attacks on the (stream) ciphers using them as nonlinear components. We shall investigate a general construction of Boolean functions f from vectorial functions, in which the support of f equals the image set of an injective vectorial function F, that we call a parameterization of f. We shall propose several derived constructions providing good trade-offs between cryptographic security and speed.